

# Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation

Mark Hillery<sup>1,2</sup>

<sup>1</sup>*Department of Physics, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10065 USA*

<sup>2</sup>*Physics Program, Graduate Center of the City University of New York, 365 Fifth Avenue, New York, NY 10016*

That superpositions of states can be useful for performing tasks in quantum systems has been known since the early days of quantum information, but only recently has a quantitative theory of quantum coherence been proposed. Here we apply that theory to an analysis of the Deutsch-Jozsa algorithm, which depends on quantum coherence for its operation. The Deutsch-Jozsa algorithm solves a decision problem, and we focus on a probabilistic version of that problem, comparing probability of being correct for both classical and quantum procedures. In addition, we study a related decision problem in which the quantum procedure has one-sided error while the classical procedure has two-sided error. The role of coherence on the quantum success probabilities in both of these problems is examined.

PACS numbers: 03.65.Yz, 03.67.Ac

## I. INTRODUCTION

It is well known that entanglement is a resource that can be used for a number of tasks, for example, teleporting a quantum state from one system to another. More recently, other quantum properties have been explored as resources. The most recent is coherence [1]. Coherence is a basis-dependent property, and it depends on the off-diagonal matrix elements of the density matrix expressed in that basis. The standard example is that of a particle going through an interferometer. In order to see an interference pattern at the output, there has to be coherence between the paths the particle can take inside the interferometer. One way to decrease the coherence between the paths is to gain information about which path the particle took, and doing so decreases the visibility of the interference pattern [2]-[8]. In [1] two different ways of quantifying coherence were proposed, and we shall make use of one of them.

In order to treat a property, such as entanglement or coherence, as a resource, one needs a measure in order to quantify how much of that resource one has. In the case of a pure, bipartite entangled state, the von Neumann entropy of one of the reduced density matrices of the state has proven to be a useful measure. In the case of coherence, one defines a set of incoherent states (this set is basis-dependent), and the coherence of a state can be characterized by its distance from this set. In [1], several possible distances were explored, and two with particularly nice properties were singled out. One is based on relative entropy, and the other on the  $l_1$  norm of the density matrix. Here we shall use the latter.

In the context of coherence as a resource, it is useful to see how the performance of a quantum algorithm that depends on coherence changes as the amount of coherence in the system decreases. One of the first quantum algorithms, the Deutsch-Jozsa algorithm, depends on quantum coherence for its operation, and it is particularly simple [9]. In fact, it can be rephrased as a particle

going through a multi-arm interferometer and looking at the interference pattern at the output. We will use a quantum walk version of the Deutsch-Jozsa algorithm to show this. The Deutsch-Jozsa algorithm solves a decision problem and does the following. One is given an oracle that evaluates a Boolean function, which is promised to be constant or balanced, and one's task is to determine which. We will assume that our Boolean function maps  $n$ -bit strings to either 0 or 1, and if the input to the oracle is the string  $x$ , its output is  $f(x)$ . A constant function is the same on all inputs and a balanced one is 0 on half of the inputs and 1 on the others. In the worst case scenario, one would have to check  $2^{n-1} + 1$  inputs to be certain which kind of function one had, while in the quantum case only one function evaluation is necessary.

If one is willing to accept a probabilistic answer, classically one would only have to check a few inputs in order to determine which type of function the oracle represented with a small probability of making a mistake. Consequently, the Deutsch-Jozsa algorithm is not a practical one, but it does serve to illustrate how quantum mechanics allows one to perform tasks in a different way than would be possible on a classical computer, and gain some quantum advantage. The classical-quantum comparison can be made precise by asking for the probability of obtaining the correct answer, constant or balanced, in a fixed number of runs.

Here we wish to examine the effect of decoherence on the performance of the Deutsch-Jozsa algorithm, and a variant of it, using a recently defined measure of coherence [1]. The Deutsch-Jozsa algorithm depends on quantum coherence, and the less of it there is, the worse the algorithm will perform. We wish to make this statement quantitative using one of the measures for coherence proposed in [1] and several different measures for the performance of the algorithm. We will see how the amount of coherence affects our ability to distinguish the balanced and constant cases for a fixed number of measurements and compare this to the result of a classical procedure. We will then examine modified decision prob-

lem, deciding between a balanced function and one that is biased, i.e.  $\sum_x f(x) = \epsilon 2^n$ , where  $\epsilon$  is known.

## II. QUANTUM WALK

We will use a quantum walk version of the Deutsch-Jozsa algorithm. The reason for doing so is that this version of the algorithm shows that the Deutsch-Jozsa algorithm is analogous to sending a particle through an interferometer that has a large number of paths. This use of the interferometer makes it clear that the quantum resource we are using is just quantum coherence. The graph on which the walk takes place is shown in Figure 1. The tails on the graph are semi-infinite, with the right-hand tail having vertices  $N+1, N+2, \dots$ , and the left-hand tail having vertices  $0, -1, -2$ , and so on. We will be using a scattering walk, which is a discrete-

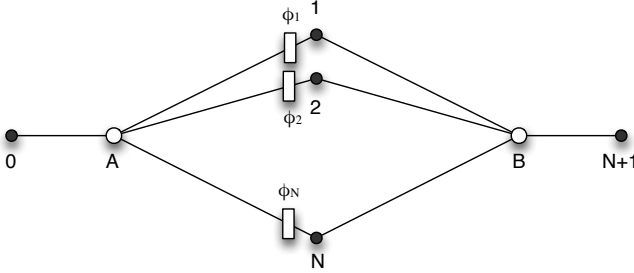


FIG. 1: Graph on which the quantum walk takes place. The vertices  $A$  and  $B$  are Fourier vertices, and all other vertices simply transmit the particle. There are  $N$  paths going from vertex  $A$  to vertex  $B$ . The rectangles are phase shifters and the  $j^{\text{th}}$  one multiplies the state by  $\exp(i\phi_j)$ . The tails, one starting at the vertex  $0$  and the other starting at the vertex  $N+1$ , are semi-infinite.

time quantum walk [10]. In this type of walk, the particle sits on the edges, not the vertices, and each edge has two orthogonal states, each corresponding to the particle moving in a particular direction. For example, the edge between  $0$  and  $A$  has the states  $|0, A\rangle$  corresponding to the particle being on that edge and moving from  $0$  to  $A$ , and the state  $|A, 0\rangle$  corresponding to the particle being on that edge and moving from  $A$  to  $0$ . To each vertex of the graph corresponds a unitary operator that transforms states entering the vertex into states leaving the vertex. The unitary operator that advances the walk one time step is composed of the combined actions of the unitary operators at the individual vertices. The vertices  $A$  and  $B$  are Fourier transform vertices and the unitary operators corresponding to them,  $U_A$  and  $U_B$  respectively, act

as

$$U_A|j, A\rangle = \frac{1}{\sqrt{N+1}} \sum_{k=0}^N e^{2\pi jk/(N+1)} |A, k\rangle$$

$$U_B|j, B\rangle = \frac{1}{\sqrt{N+1}} \sum_{k=1}^{N+1} e^{2\pi jk/(N+1)} |B, k\rangle. \quad (1)$$

The other vertices just transmit the particle, but those with a phase shifter also add a phase factor to the transmitted state,

$$|A, j\rangle \rightarrow e^{i\phi_j} |j, B\rangle. \quad (2)$$

In our case the phases,  $\phi_j$ , will be either  $0$  or  $\pi$ , and these phases correspond to the output of the Boolean function in the Deutsch-Jozsa algorithm. The phases are promised either to be all the same (constant) or half of them are  $0$  and half are  $\pi$  (balanced). Our task is to find out which of the two cases we have. We will start the particle in the state  $|0, A\rangle$ , run the walk for 3 steps, and then see whether or not it is in the state  $|B, N+1\rangle$ . If we find the particle in that state we will conclude the phases were all the same, and if we do not, we will conclude we had the balanced situation.

In order to compare the quantum walk result to a classical one, we will assume that classically we are able to sample the phase shifters, i.e. pick some of them and see how they are set, whether to  $0$  or  $\pi$ . Then a classical versus quantum comparison will consist of a comparison between the number of phase shifters we sample versus the number of times we have to run the quantum walk.

## III. ANALYSIS OF THE WALK

We start the particle making the walk in the state  $|0, A\rangle$ . After two steps, its state is

$$\frac{1}{\sqrt{N+1}} \left[ |0, -1\rangle + \sum_{j=1}^N e^{i\phi_j} |j, B\rangle \right]. \quad (3)$$

One more step yields the state

$$\frac{1}{\sqrt{N+1}} |-1, -2\rangle + \frac{1}{N+1} \sum_{j=1}^N \sum_{k=1}^N e^{i\phi_j} e^{2\pi ijk/(N+1)} |B, k\rangle + \frac{1}{N+1} \left( \sum_{j=1}^N e^{i\phi_j} \right) |B, N+1\rangle. \quad (4)$$

The last term is the one that interests us, because it yields the probability that the particle is on the edge between  $B$  and  $N+1$ . If all of the phases,  $\phi_j$  are the same, this probability is just  $N^2/(N+1)^2$ , and if half the

phases are 0 and half  $\pi$ , then, assuming  $N$  is even, it is zero. Therefore, with a small error of order  $1/N$ , which we shall assume we can neglect, we can determine which of these two possibilities we have by measuring the walk after three steps to see whether the particle is between  $B$  and  $N+1$  or not.

Now we want to introduce decoherence into this system. One way of doing so is to introduce a qubit for each leg of the graph. In particular, let us suppose that all of these qubits are initially in the state  $|0\rangle$ . When the particle goes through the vertex  $j$ , in addition to picking up the phase  $e^{i\phi_j}$ , the  $j^{\text{th}}$  qubit goes from the state  $|0\rangle_j$  to the state  $|\mu_j\rangle_j$ , which is a linear combination of the states  $|0\rangle_j$  and  $|1\rangle_j$ ,  $|\mu_j\rangle_j = \alpha_j|0\rangle_j + \beta_j|1\rangle_j$ . If we let

$$|\eta_j\rangle = |\mu_j\rangle_j \prod_{k=1, k \neq j}^N |0\rangle_k, \quad (5)$$

for  $j = 1, 2, \dots, N$  and  $|\eta_0\rangle = \prod_{k=1}^N |0\rangle_k$ , then the state after two steps is

$$\frac{1}{\sqrt{N+1}} \left[ |0, -1\rangle |\eta_0\rangle + \sum_{j=1}^N e^{i\phi_j} |j, B\rangle |\eta_j\rangle \right]. \quad (6)$$

The reduced density matrix corresponding to this state, where we trace out the ancilla qubits, is given by

$$\begin{aligned} \rho_{int} &= \frac{1}{N+1} \sum_{j=1}^N \sum_{k=1}^N e^{i(\phi_j - \phi_k)} \langle \eta_k | \eta_j \rangle |j, B\rangle \langle k, B| \\ &\quad + O(N^{-1/2}). \end{aligned} \quad (7)$$

One of the measures of coherence defined in [1] for a general density matrix,  $\rho$ , on an  $M$ -dimensional space is

$$C_{l_1}(\rho) = \sum_{i,j=1, i \neq j}^M |\rho_{ij}|. \quad (8)$$

If we define

$$X = \frac{1}{(N+1)^2} \sum_{j,k=1, j \neq k}^N |\langle \eta_k | \eta_j \rangle|, \quad (9)$$

then we see that

$$C_{l_1}(\rho_{int}) = (N+1)X + O(N^{-1/2}). \quad (10)$$

Note that in the case in which all of the qubit states  $|\mu_j\rangle_j$  are the same, then the inner products  $\langle \eta_k | \eta_j \rangle$  are independent of  $j$  and  $k$  for the case  $j \neq k$ . Setting  $\nu = |\langle \eta_k | \eta_j \rangle|$ , we then find that  $X = \nu N(N-1)/(N+1)^2$ . If we now let the walk go one more step, the state is

$$\begin{aligned} &\frac{1}{\sqrt{N+1}} |-1, -2\rangle |\eta_0\rangle \\ &+ \frac{1}{N+1} \sum_{j=1}^N \sum_{k=1}^N e^{i\phi_j} e^{2\pi i j k / (N+1)} |B, k\rangle |\eta_j\rangle \\ &+ \frac{1}{N+1} \left( \sum_{j=1}^N e^{i\phi_j} |\eta_j\rangle \right) |B, N+1\rangle. \end{aligned} \quad (11)$$

Forming a density matrix from this state and tracing out the ancillas gives us the output density matrix for the particle making the walk,  $\rho_{out}$ , and the probability of finding the particle on the edge between  $B$  and  $N+1$  is

$$\begin{aligned} \langle B, N+1 | \rho_{out} | B, N+1 \rangle &= \frac{1}{(N+1)^2} \\ &\quad \left( \sum_{j=1}^N \sum_{k=1}^N e^{i(\phi_j - \phi_k)} \langle \eta_k | \eta_j \rangle \right). \end{aligned} \quad (12)$$

Note that

$$\langle B, N+1 | \rho_{out} | B, N+1 \rangle \leq \frac{N}{(N+1)^2} + X. \quad (13)$$

What this tells is that the amount of coherence in the system places an upper limit on our ability distinguish the constant and balanced cases. With perfect coherence the particle always (up to  $O(1/N)$ ) finishes in the state  $|B, N+1\rangle$  and in the balanced case it never does. When the amount of coherence decreases, the the probability that the constant case will be mistaken for the balanced case increases. This shows that the quantum resource that is being used to accomplish this task is coherence.

#### IV. DEUTSCH-JOZSA ALGORITHM

Now let us see what happens to the results of the Deutsch-Jozsa algorithm as the amount of coherence in the system is decreased in more detail. In particular, we will examine the probability of correctly identifying whether the interferometer is constant or balanced in a fixed number of runs. We shall look at the case that  $\langle \eta_k | \eta_j \rangle$  is independent of  $j$  and  $k$  for  $j \neq k$  and we shall assume the inner product is real and positive so we can set  $\langle \eta_k | \eta_j \rangle = |\langle \eta_k | \eta_j \rangle| = \nu$ . If all of the  $\phi_j$  are the same, then

$$\begin{aligned} \langle B, N+1 | \rho_{out} | B, N+1 \rangle &= \frac{1}{(N+1)^2} [N + \nu N(N-1)] \\ &\simeq \nu + O(1/N). \end{aligned} \quad (14)$$

If half of the  $\phi_j$  are 0 and half are  $\pi$ , then we have that

$$\begin{aligned} \langle B, N+1 | \rho_{out} | B, N+1 \rangle &= \frac{1}{(N+1)^2} [(1-\nu)N \\ &\quad + \nu \sum_{j,k=1}^N e^{i(\phi_j - \phi_k)}] \\ &= \frac{(1-\nu)N}{(N+1)^2} \\ &= O(1/N). \end{aligned} \quad (15)$$

Our procedure is to run the walk and measure whether the particle is in the state  $|B, N+1\rangle$ . If it is, we guess that we have the constant case, and if not, we guess we

have the balanced case. We see that as the amount of coherence decreases, our chance of making an error increases. Note that the error is almost one-sided. If the particle comes out, we know with very high probability that all of the  $\phi_j$  are the same. However, if it does not come out, and we guess that the  $\phi_j$  are in the balanced configuration, then, assuming the balanced and constant cases are equally likely, we have a chance of  $(1 - \nu)/2$  of being wrong. Classically, looking at one of the phase shifters gives us no information about which of the two cases we have, so for one trial, the quantum case does better. Clearly, coherence is a resource in the quantum case, because the more coherence there is in the system, the less likely we are to make a mistake.

Now let's see what happens with two trials. Let's look at the classical case first. We shall call the results of the trials  $y_1$  and  $y_2$ , where  $y_j = \pm 1$ . Here we are denoting the phase shifters by  $e^{i\phi}$  rather than  $\phi$ , so a phase of 0 corresponds to 1 and a phase of  $\pi$  corresponds to  $-1$ . There are four possible results,  $(y_1, y_2)$ , if we sample two of the phase shifters,  $(1, 1)$ ,  $(1, -1)$ ,  $(-1, 1)$ , and  $(-1, -1)$ . We will assume that the balanced and constant cases are equally likely, and that within the constant category, each value is equally likely. If the results are different we know we have the balanced case. This happens with a probability of  $1/4$  (the probability of the results being different). If we get the same result for each trial, things get a bit more complicated. We want to find  $P(c|y_1 y_2)$ , the probability that we have the constant case given that we have the result  $(y_1, y_2)$ , and similarly  $P(b|y_1, y_2)$ , the probability that we have the balanced case. Clearly  $P(b|1, -1) = P(b|-1, 1) = 1$ . To find the probabilities when the results are the same, we use Bayes' theorem. Let us find  $P(c|1, 1) = P(c = 1|1, 1)$ , where we have specifically indicated which constant value the phase shifter will have. We then have

$$P(c = 1|1, 1) = \frac{P(1, 1|c = 1)P(c = 1)}{P(1, 1)}. \quad (16)$$

Now  $P(1, 1|c = 1) = 1$  and  $P(c = 1) = 1/4$ . For the denominator we have

$$\begin{aligned} P(1, 1) &= P(1, 1|c = 1)P(c = 1) + P(1, 1|b)P(b) \\ &= \frac{3}{8}. \end{aligned} \quad (17)$$

Finally, this gives us that  $P(c|1, 1) = 2/3$ , which implies that  $P(b|1, 1) = 1/3$ . Similarly,  $P(c|-1, -1) = 2/3$ . Our strategy, then, is to guess balanced if the results are different, and constant, if they are the same. Our probability of being correct is  $3/4$ , i.e. we are always correct if the results are different and are correct with a probability  $2/3$  when they are the same.

Now let us look at the quantum case. We run the walk twice, and we denote the results of the runs by  $(0, 0)$ ,  $(1, 0)$ ,  $(0, 1)$  and  $(1, 1)$ , where 0 denotes we did not find the particle in the state  $|B, N+1\rangle$  and 1 indicates that

we did. Neglecting terms of  $O(1/N)$ , we have that

$$\begin{aligned} P(0, 0|c) &= (1 - \nu)^2 \\ P(0, 1|c) &= P(1, 0|c) = \nu(1 - \nu) \\ P(1, 1|c) &= \nu^2, \end{aligned} \quad (18)$$

and  $P(0, 0|b) = 1$  and  $P(0, 1|b) = P(1, 0|b) = P(1, 1|b) = 0$ . Now making use of Bayes' theorem we have that in the cases  $(1, 0)$ ,  $(0, 1)$  and  $(1, 1)$ , we can conclude that we have the constant case with certainty. If we obtain  $(0, 0)$ , then we have

$$\begin{aligned} P(c|0, 0) &= \frac{(1 - \nu)^2}{(1 - \nu)^2 + 1} \\ P(b|0, 0) &= \frac{1}{(1 - \nu)^2 + 1}. \end{aligned} \quad (19)$$

Now the first of these probabilities is less than or equal to the second, so if our measurement results are  $(0, 0)$ , we should always guess balanced. In all other cases we guess constant. Doing so, our probability of being wrong is  $(1/2)(1 - \nu)^2$ . The quantum error probability will be less than the classical one when

$$\frac{1}{2}(1 - \nu)^2 < \frac{1}{4}, \quad (20)$$

or  $\nu > (\sqrt{2} - 1)/\sqrt{2}$ . So in the case of two trials, as long as the amount of decoherence is not too great, the quantum method is better.

This can be generalized to  $m$  trials for  $m \ll N$ . Before doing so, let us be more careful about specifying our ensemble. We are assuming that each of the constant cases occurs with probability  $1/4$ , and that the total probability of the balanced case is  $1/2$ . Within the balanced case, each of the balanced sequences has the same probability. So far, we have assumed that, given the balanced case, this is equivalent to the probability that a particular phase shifter has  $y_j = 1$  is  $1/2$ , the probability that it has  $y_j = -1$  is  $1/2$ , and that different phase shifters can be treated as independent. This needs to be justified, and this is done in the Appendix. We find that as long as  $m \ll N$ , this assumption is valid.

In the classical case, the only ambiguous situation is if all of the examined phase shifters are found to be the same. We would then guess that we are in the constant situation. In the quantum case, the only ambiguous case is if the particle is never found between  $B$  and  $N+1$ . We would then guess that we are in the balanced situation. Let us have a look at these cases and see what the probability of making a mistake is. In all other situations, the probability of making a mistake is very small.

We start with the classical case. Denote the probability that we have  $c = 1$  given that we examined  $m$  phase shifters and found them to be 1 by  $P(c = 1|m1)$ . Making use of Bayes' theorem and

$$\begin{aligned} P(m1) &= P(m1|c = 1)P(c = 1) + P(m1|b)P(b) \\ &= \frac{1}{4} + \frac{1}{2^{m+1}}, \end{aligned} \quad (21)$$

we find that

$$P(c = 1|m1) = \frac{2^{m-1}}{1 + 2^{m-1}}, \quad (22)$$

The result for the probability for  $c = -1$  when we found  $m$  phase shifters to be  $-1$  is the same. Since we will guess the constant case in both these situations, the probability of being wrong is

$$\begin{aligned} p_{error}^{(class)} &= 2[1 - P(c = 1|m1)]P(m1) \\ &= \frac{2}{1 + 2^{m-1}} \left( \frac{1}{4} + \frac{1}{2^{m+1}} \right) = \frac{1}{2^m}. \end{aligned} \quad (23)$$

Now we move to the quantum case, and  $P(c|m0)$  now denotes the probability that we have the constant case given that the particle was not found in the state  $|B, N+1\rangle$  in  $m$  trials. Now application of Bayes' theorem and the fact that

$$\begin{aligned} P(m0) &= P(m0|c)P(c) + P(m0|b)P(b) \\ &= \frac{1}{2}(1 - \nu)^m + \frac{1}{2} \end{aligned} \quad (24)$$

gives us

$$P(c|m0) = \frac{(1 - \nu)^m}{1 + (1 - \nu)^m}. \quad (25)$$

Now in this case we will guess balanced, so the probability of being wrong is

$$p_{error}^{(quant)} = P(c|m0)P(m0) = \frac{1}{2}(1 - \nu)^m. \quad (26)$$

If  $\nu > 1 - (2^{1/m}/2)$ , then we will have  $p_{error}^{(quant)} < p_{error}^{(class)}$ . This tells us how much coherence we need for the quantum method to outperform the classical one.

## V. VARIATION ON DEUTSCH-JOZSA

The decision problem we looked at in the previous section was one in which both the quantum algorithm and the classical one had (almost) one-sided error. In the classical case, if the interferometer is constant, we will never guess balanced, and in the quantum case, if it is balanced, we will never guess constant. Here we would like to look at a situation in which the quantum algorithm has one-sided error, but the classical one does not. This can give the quantum algorithm a significant advantage if the errors have different costs. We again look at the case where the phase shifts are either 0 or  $\pi$ , but we now want to distinguish between the case in which the phase shifts are balanced and the case in which

$$\frac{1}{N} \sum_{j=1}^N e^{i\phi_j} = \epsilon, \quad (27)$$

where we assume that  $\epsilon \ll 1$ . In order to distinguish between these alternatives, our strategies are the same as

before. The quantum strategy is to run a quantum walk a certain number of times, and the classical strategy is to sample the phase shifters.

In this case, the quantum strategy is the easier one to analyze. Let us first consider the situation without decoherence. We know that in the balanced case, the probability of measuring the particle to be in the state  $|B, N+1\rangle$  after the walk is, up to  $O(1/N)$ , zero. In the second case, which we shall refer to as the  $\epsilon$  case, the probability to find the particle in that state is  $\epsilon^2$ . In that case, if the walk is run  $m$  times, the probability of not finding the particle between  $B$  and  $N+1$  is

$$(1 - \epsilon^2)^m \simeq e^{-m\epsilon^2}, \quad (28)$$

where we have made use of the fact that  $\ln(1 - \epsilon^2)^m \simeq -m\epsilon^2$ . Therefore, in order to detect this case, that is to find the particle at least once in the state  $|B, N+1\rangle$ , we need  $m\epsilon^2$  to be at least of order 1. Our strategy is to assume that if we ever find the particle in the state  $|B, N+1\rangle$  in  $m$  runs that we have the  $\epsilon$  case, and that we have the balanced case otherwise. If we are given the balanced case, we will always be correct, and if we are given the  $\epsilon$  case and  $m\epsilon^2$  is of order 1 or greater, our probability of error will also be small. If there is decoherence, the effect is simply to replace  $\epsilon^2$  by  $\nu\epsilon^2$ , so that as long as  $\nu$  is not too small, the effect of decoherence will not be large.

Now we turn to the classical case. We will look at  $m$  of the phase shifters. Let each sampled phase shifter be represented by a variable  $y_j$ , where  $y_j = 1$  corresponds to  $\phi_j = 0$  and  $y_j = -1$  corresponds to  $\phi_j = \pi$ . We define

$$Y = \frac{1}{m} \sum_{j=1}^m y_j. \quad (29)$$

If we find  $Y \geq \epsilon/2$  we shall assume that we have the  $\epsilon$  case, otherwise we will assume we have the balanced case. Therefore, we want to find the probability of making an error.

Let us start by assuming that we have the balanced case, and we would like to find the probability that we would identify it as the  $\epsilon$  case. We will assume that all of the balanced sequences of  $N$  phase shifters are equally probable. If we are only sampling  $m \ll N$  of the phase shifters, this is equivalent to assuming that each phase shifter we look at has an equal chance of having  $y_j = 1$  and  $y_j = -1$  (see Appendix). We now want to find the probability that  $Y \geq \epsilon/2$ . For this purpose we can use the Chernoff bound [11]. It states that if we have the independent random variables,  $X_j$ ,  $j = 1, 2, \dots, n$ , where  $X_j$  can be either 0 or 1, and its probability of being 1 is  $p_j$ , then for  $X_T = \sum_{j=1}^n X_j$ ,  $\mu = \sum_{j=1}^n p_j$ , and any  $\delta > 0$ , then

$$P(X_T > (1 + \delta)\mu) < \left[ \frac{e^\delta}{(1 + \delta)^{(1 + \delta)}} \right]^\mu. \quad (30)$$

In our case  $\mu = m/2$ , and setting  $X_j = (1/2)(y_j + 1)$ , we find that  $Y > \epsilon/2$  implies  $X_T > m[(\epsilon/2) + 1]/2$  so that

$$P(Y > \epsilon/2) < \left[ \frac{e^{\epsilon/2}}{(1 + \epsilon/2)^{1+\epsilon/2}} \right]^{m/2}. \quad (31)$$

Assuming  $\epsilon \ll 1$  and keeping lowest order terms in  $\epsilon$ , we find

$$\ln \left[ \frac{e^{\epsilon/2}}{(1 + \epsilon/2)^{1+\epsilon/2}} \right] \simeq -\epsilon^2/4, \quad (32)$$

so that the right-hand side of Eq. (31) is approximately  $e^{-\epsilon^2 m/8}$ .

Similarly, let us suppose that we have the  $\epsilon$  case. We will assume that all sequences of  $N$  phase shifters satisfying  $\sum_{j=1}^N y_j = \epsilon N$  are equally likely. For a subsequence of length  $m$ , where  $m \ll N$ , this is equivalent to assuming that each element has a probability of  $(1 + \epsilon)/2$  to be  $+1$  and  $(1 - \epsilon)/2$  to be  $-1$  (see Appendix). We now want to find the probability that we would identify this as the balanced case, which is the same as finding  $Y < \epsilon/2$ . We can now use the following version of the Chernoff bound [11]. With the same conditions as before,

$$P(X_T < (1 - \delta)\mu) < e^{-\mu\delta^2/2}. \quad (33)$$

We now have that  $\mu = m(1 + \epsilon)/2$  and  $Y < \epsilon/2$  implies  $X_T < m[(\epsilon/2) + 1]/2$ , which further implies that

$$\delta = \frac{\epsilon}{2(1 + \epsilon)}. \quad (34)$$

Finally, keeping only lowest order terms in  $\epsilon$ , we find that

$$P(Y < \epsilon/2) < e^{-\epsilon^2 m/8}. \quad (35)$$

Summarizing, we see the following. For both the quantum and classical methods, the condition for keeping the error small is the same,  $m\epsilon^2$  should be at least of order 1. However, up to  $O(1/N)$ , the quantum error is one-sided, if we have the balanced case, we will not mistake it for the  $\epsilon$  case. For the classical method, the error is two-sided, we can mistake each case for the other. Therefore, if we are in a situation in which the cost of mistaking the balanced case for the  $\epsilon$  case is large, the quantum method has an advantage. Note that for this situation, deciding between the balanced and  $\epsilon$  cases, the type of decoherence we are considering does not affect the fact that the quantum error is one sided, but it will cause the number of runs that we need to make in the quantum case, which is of order  $1/(\nu\epsilon^2)$ , to increase. The reason it does not affect the one-sidedness of the error, is that the decoherence respects the symmetry of the problem; it is the same for each branch of the interferometer. This suggests that for some problems for which coherence is a resource, not only its total quantity, but its properties will play a role.

## VI. CONCLUSION

We have examined the role played by coherence as a resource in the Deutsch-Jozsa and related algorithms. The Deutsch-Jozsa algorithm is a means of solving a decision problem, in particular, deciding between two alternatives. In its ideal form, it provides an answer in a single run, whereas classically in the worst case an exponential number of runs would be necessary. Decoherence degrades the ability of the algorithm to decide between the alternatives, and the smaller the amount of coherence in the system, the worse the ability of the algorithm to distinguish between the two cases. This demonstrates that coherence is a resource for this algorithm. We also looked at the Deutsch-Jozsa algorithm in a probabilistic setting, and found that as long as there is enough coherence present, there is a quantum advantage in that for a fixed number of measurements, one has a higher probability of making the correct decision using quantum means than by using classical ones. By looking at a related decision problem, we found an example in which the number of measurements one makes is comparable for the classical and quantum cases, at least if the coherence in the quantum case remains high enough, but while the classical procedure has two-sided error, the quantum procedure has one sided error.

## Acknowledgment

This research was supported by a grant from the John Templeton Foundation. I would like to thank Seth Cottle, Emilio Bagan, and Janos Bergou for useful conversations.

## Appendix

We now need to justify what we did in Sections III and IV. In the our ensemble in Section III, each balanced sequence of length  $N$  occurred with equal probability. A related ensemble occurred in Section IV. We want to show the following. We consider an ensemble of sequences of length  $N$  consisting of  $\pm 1$ , in which each sequence has  $pN$  ones and  $(1 - p)N$  minus ones. Each of these sequences has the same probability. We now consider fixed subsequences of these sequences of length  $m$ , e.g. the first  $m$  elements of each sequence of length  $N$ . We want to show that the probability of a subsequence with  $m_+$  ones and  $m_-$  minus ones, where  $m_+ + m_- = m$ , is the same as if each location in the subsequence has a probability  $p$  of containing a one and a probability  $1 - p$  of containing a minus one.

For convenience, we will consider subsequences consisting of the first  $m$  places of the sequences of length  $N$ . The probability,  $p(m_+, m_-)$  that the subsequence

has  $m_+$  ones is

$$\begin{aligned} p(m_+, m_-) &= \frac{\binom{m}{m_+} \binom{N-m}{pN-m_+}}{\binom{N}{pN}} \\ &= \binom{m}{m_+} F, \end{aligned} \quad (36)$$

where

$$F = \frac{(N-m)!(pN)!(N-pN)!}{N!(pN-m_+)(N-pN-m_+)!}. \quad (37)$$

Now we shall assume that  $m$  is much less than  $N$ ,  $pN$ , and  $(1-p)N$  and apply the Stirling approximation,  $n! \simeq \sqrt{2\pi n} n^n e^{-n}$ . We then have

$$\frac{(N-m)!}{N!} \simeq \sqrt{1 - \frac{m}{N}} \frac{e^m}{N^m} \left(1 - \frac{m}{N}\right)^{N-m}. \quad (38)$$

We can approximate the last factor by taking its logarithm and expanding in  $m/N$

$$\begin{aligned} \ln \left(1 - \frac{m}{N}\right)^{N-m} &= (N-m) \left(-\frac{m}{N} - \frac{m^2}{2N^2} + \dots\right) \\ &= -m - \frac{m^2}{2N} + O(m/N). \end{aligned} \quad (39)$$

This gives us

$$\frac{(N-m)!}{N!} \simeq \sqrt{1 - \frac{m}{N}} \frac{1}{N^m} e^{-m^2/2N}. \quad (40)$$

Applying this relation to  $(pN-m_+)!/(pN)!$  and  $[(1-p)N - (m-m_+)]!/[(1-p)N]!$  and substituting into the expression for  $F$ , we obtain

$$F \simeq p^{m_+} (1-p)^{m-m_+} + O(m/\sqrt{N}). \quad (41)$$

This gives us

$$p(m_+, m_-) \simeq \binom{m}{m_+} p^{m_+} (1-p)^{m-m_+}, \quad (42)$$

which is what we would obtain if we assumed that in the sequence of length  $m$  one occurred with probability  $p$  and minus one occurred with probability  $1-p$ .

- 
- [1] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).
  - [2] D. M. Greenberger and A. YaSin, Phys. Lett. A **128**, 391 (1988).
  - [3] G. Jaeger, A. Shimony, and L. Vaidman, Phys. Rev. A **51**, 54 (1995).
  - [4] B.-G. Englert, Phys. Rev. Lett. **77**, 2154 (1996).
  - [5] S. Dürr, Phys. Rev. A **64**, 042113 (2001).
  - [6] B.-G. Englert and J. Bergou, Opt. Commun. **179**, 337 (2000).
  - [7] M. Jakob and J. A. Bergou, Phys. Rev. A **76**, 052107 (2007).
  - [8] M. N. Bera, T. Qureshi, M. A. Siddiqui, and A. K. Pati, Phys. Rev. A **92**, 012118 (2015).
  - [9] D. Deutsch and R. Jozsa, Proc. Royal Soc. London A **439**, 553 (1992).
  - [10] M. Hillery, J. Bergou, and E. Feldman, Phys. Rev. A **68**, 032314 (2003).
  - [11] R. Motwani and P. Raghavan, *Randomized Algorithms*, (Cambridge University Press, Cambridge, 1995).